

REMARKS

Reconsideration of this application, as amended, is earnestly requested.

Claims 1, 5, 9-10, 18, and 21-22 are amended as shown above; claims 6-8, 14-17, 19-20, and 24 are cancelled without prejudice; and claim 4 previously has been cancelled without prejudice. Claims 1-3, 9-13, 18, 21-23, and 25-27 remain pending in the application with claims 1, 10, 22, and 25 being independent claims.

Claims 1-2, 5-7, 9-11, and 14-24 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Wasilewski (US 5,420,866) in view of Daemen ("AES Proposal: Rijndael," March 1999), claims 3 and 12-13 as being unpatentable over Wasilewski in view of Daemen and further in view of Mroczkowski ("Implementation of the block cipher Rijndael using Altera FPGA," May 2000), and claims 25-27 as being unpatentable over Wasilewski in view of Daemen and further in view of Vanstone (US 6,212,281). Claims 1, 10, and 22 stand rejected under 35 U.S.C. §101 as being directed to non-statutory subject matter. Further claims 1, 10, and 22 stand rejected under 35 U.S.C. §112, first paragraph, for failing to comply with the written description requirement. Claim 8 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base and any intervening claims. These rejections are respectfully traversed.

Applicant appreciates the acknowledgement of allowable matter.

Applicant amends independent claim 1 to include the allowable limitation of dependent claim 8 and the limitations of intervening claims 6-7. Independent claims 10 and 22 have been similarly amended.

In amending claims 1, 10, and 22, applicant has addressed the 112 rejection in which "key schedule" was not an output of the key schedule unit. The phrase "key" schedule" has been replaced by "round key" which is specifically

mentioned in the specification at paragraph 0035. Applicant has also addressed the Examiner's comment that the specification does is silent on storing expanded keys.

Applicant respectfully requests reconsideration and withdrawal of the 103 and 112 rejections as they pertain to independent claims 1, 10, and 22. Additionally, claims 2-3, 9, 11-13, 18, 21 and 23 are patentable at least by virtue of dependence upon a patentable independent claim.

Regarding the Examiner's 101 rejections, MPEP 2106 IV.C.2 indicates that to satisfy section 101 requirements, the claim must be for a practical application of an § 101 judicial exception, which can be identified in various ways:

- (1) the claimed invention "transforms" an article or physical object to a different state or thing, or
- (2) the claimed invention otherwise produces a useful, concrete and tangible result.

Applicant submits that the claimed invention meets of both of these requirements, even though only one is necessary to establish compliance with section 101.

It is well settled that the claim shall be reviewed to determine if it provides a transformation or reduction of an article to a different state or thing. If such a transformation or reduction is found, the inquiry ends because the claim meets the statutory requirement of 35 U.S.C. § 101. (MPEP 2106 IV.C.2(1)).

Claim 1 is directed towards "an apparatus for encrypting/decrypting a real-time input stream" and recites the elements of a control unit, a key schedule unit, and a block round unit. Using the language of the MPEP, the control unit receives a data stream, and the data stream is transformed by the key schedule unit and the block round unit to provide an encrypted or decrypted data blocks

back to the control unit. Simply put, an encrypted data stream that is received by the control unit is transformed into decrypted data blocks and this transformation meets the statutory requirements of section 101.

Further, claim 1 also meets the second prong of the test that the claim is a practical application of a section 101 judicial exception. Claim 1 produces a useful, concrete, and tangible result.

For an invention to be “useful” it must satisfy the utility requirement of section 101. The USPTO's official interpretation of the utility requirement provides that the utility of an invention has to be (i) specific, (ii) substantial and (iii) credible. (MPEP 2107). In the present application, there is no question that utility exists. Claim 1 is directed to an apparatus for decrypting or encrypting a stream of data, which results in the generation decrypted or encrypted data blocks. The “usefulness” element is clearly met.

Another consideration is whether the claimed invention produces a “concrete” result. Usually, this question arises when a result cannot be assured. In other words, the process must have a result that can be substantially repeatable or the process must substantially produce the same result again. *In re Swartz*, 232 F.3d 862, 864, 56 USPQ2d 1703, 1704 (Fed. Cir. 2000) (where asserted result produced by the claimed invention is “irreproducible” claim should be rejected under section 101).

In the present application, claim 1 recites a combination of elements. Applicant submits that one practicing the recited invention will be able to repeatedly generate encrypted or decrypted data blocks by using the various elements recited in the claim. No undue experimentation is necessary. Given the same or a similar data stream, as well as the same or similar parameters recited in the claim, the various elements of this claim will substantially produce the same resulting encrypted or decrypted data blocks. The results of the claim are therefore reproducible, thus satisfying the concrete result element.

In *State Street*, the Federal Circuit examined some of its prior section 101 cases, observing that the claimed inventions in those cases were each for a “practical application of an abstract idea” because the elements of the invention operated to produce a “useful, concrete and tangible result.” *State Street Bank & Trust Co. v. Signature Financial Group Inc.*, 149 F. 3d 1368, 1373-74, 47 USPQ2d 1596, 1602-02 (Fed. Cir. 1998). For example, the court in *State Street* noted that the claimed invention in *Alappat* “constituted a practical application of an abstract idea (a mathematical algorithm, formula, or calculation), because it produced ‘a useful, concrete and tangible result’—the smooth waveform.” *Id.* Similarly, the claimed invention in *Arrhythmia* “constituted a practical application of an abstract idea (a mathematical algorithm, formula, or calculation), because it corresponded to a useful, concrete and tangible thing—the condition of a patient’s heart.” *Id.*

In the present matter, the practical application of claim 1 relates to the generation of an encrypted or a decrypted data blocks. Applicant submits that several elements recited in claim 1 may be interpreted as including an abstract idea such as a mathematical algorithm, formula, or calculation. In this regard, the claim is similar to the claims addressed in both the *Alappat* and *Arrhythmia* matters and noted by the court in *State Street*. However, claim 1 recites more than this abstract idea and produces a tangible result, the encrypted or decrypted stream blocks. These “encrypted or decrypted data blocks” are analogous to the “smooth waveform” in *Alappat*. In accordance with Federal Circuit precedent, the result of claim 1 (“encrypted or decrypted data blocks”) has a practical application. Thus, the tangible result element has also been met.

In summary, the applicant has demonstrated that in claim 1, a encrypted data stream is transformed into decrypted data blocks. This transformation meets the statutory requirement of 35 U.S.C. § 101. The applicant has further demonstrated that claim 1 includes a “practical application” since the final result achieved by this claim (e.g., decrypted data blocks) is “useful, tangible and concrete.” If a claim is directed to a practical application of a § 101 judicial

exception and produces a result tied to the physical world that does not preempt the judicial exception, then the claim meets the statutory requirement of 35 U.S.C. § 101. (See, MPEP 2106.IV.C.1, "The conclusion that a particular claim includes a 35 U.S.C. 101 judicial exception does not end the inquiry because the practical application of a judicial exception may qualify for patent protection.") Since claim 1 meets the practical application requirement, this claim is directed toward statutory subject matter in accordance with section 101 for this additional reason.

Independent claims 10 and 22 contain language similar to independent claim 1, and therefore these claims are also believed to be directed toward statutory subject matter for reasons similar to those presented above in conjunction with claim 1.

The Examiner also rejects claims 25-27 under section 101 stating that "propagating signals are not patentable subject matter." Applicant believes that claim 25 meets both the transformation test and produces a useful, concrete and tangible result. Claim 25 relates to controlling a data protection key comprising "generating a data key ... according to at least one of a predetermined period and a scheduled period, wherein the scheduled period depends on a change of the data key size" and "checking validity of the data key." The invention of claim 25 takes as an input a predetermined or a scheduled period and generates a data key. This meets the "transforming test." Claim 25 clearly produces a useful, concrete and tangible result in that a data key, useful for encrypting or decrypting data, can be repeatedly produced under the described conditions.

When evaluating the scope of a claim, every limitation in the claim must be considered. A claimed invention may not be dissected into discrete elements and then the elements evaluated in isolation. Instead, the claim as a whole must be considered. See, *e.g.*, *Diamond v. Diehr*, 450 U.S. 175, 188-89, 209 USPQ 1, 9 (1981) ("In determining the eligibility of respondents' claimed process for patent protection under § 101, their claims must be considered as a whole. It is

inappropriate to dissect the claims into old and new elements and then to ignore the presence of the old elements in the analysis. This is particularly true in a process claim because a new combination of steps in a process may be patentable even though all the constituents of the combination were well known and in common use before the combination was made.").

For the reasons stated above, applicant believes that claim 25 is directed to statutory subject matter.

Applicant respectfully requests reconsideration and withdrawal of the section 101 rejections.

Regarding the 103 rejection of claim 25, the Examiner has not cited any of the references that teach "generating a data key ... according to at least one of a predetermined period and a scheduled period, wherein the scheduled period depends on a change of the data key size."

Further, the Examiner cites Vanstone for teaching "checking validity of the data key." A close inspection of the cited portions of Vanstone indicates that Vanstone teaches a hash function. A hash function is a transformation that takes an input string and returns a fixed-size string, which is called the hash value. Any change in the input string will produce a different hash value. Calculating a hash value of a data string is different than "checking the validity of the data key."

Since the data key is generated according to a predetermined period or a scheduled period depending on a change of the data key size, the data key may be checked to determine whether the data key was properly generated, in other words, whether the data key meets the requirements for the data key.

The data key may also be compared with a master key stored in memory to determine whether the data key matches the master key, and if so, the data key is valid.

Neither of these "checking the validity of the data key" involves using a hash function to generate a hash value as taught by Vanstone.

As set forth in MPEP 2143, to show a *prima facie* case for obviousness, all the prior art references, either individually or combined, must teach all the claim limitations. None of the prior art, individually or in combination, teaches "generating a data key ... according to at least one of a predetermined period and a scheduled period, wherein the scheduled period depends on a change of the data key size." Applicant submits that a *prima facie* case for obviousness has not been shown and that claim 25 is patentable over the cited prior art. Additionally, claims 26-27 are patentable at least by virtue of dependence upon a patentable independent claim.

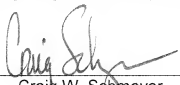
In view of the above amendments and remarks, applicants respectfully request reconsideration and withdrawal of the rejections, and an early indication of the allowance of the claims. Applicants believe the claims are in a condition for allowance and respectfully solicit favorable action.

CONCLUSION

In view of the above, reconsideration and allowance of this application are now believed to be in order, and such actions are hereby solicited. If any points remain at issue which the Examiner feels may be best resolved through a telephone interview, the Examiner is kindly invited to contact the undersigned at (213) 623-2221.

Respectfully submitted,
Lee, Hong, Degerman, Kang & Waimey

Date: November 17, 2008

By: 
Craig W. Schmoyer
Registration No. 51,007
Attorney for Applicant(s)

Customer No. 035884